



DEUTSCHES
PATENTAMT



DE 3432721 A1

⑳ Aktenzeichen: P 34 32 721.5
㉔ Anmeldetag: 6. 9. 84
㉕ Offenlegungstag: 6. 3. 86

㉗ Anmelder:
Hahn, Rüdiger, 8000 München, DE

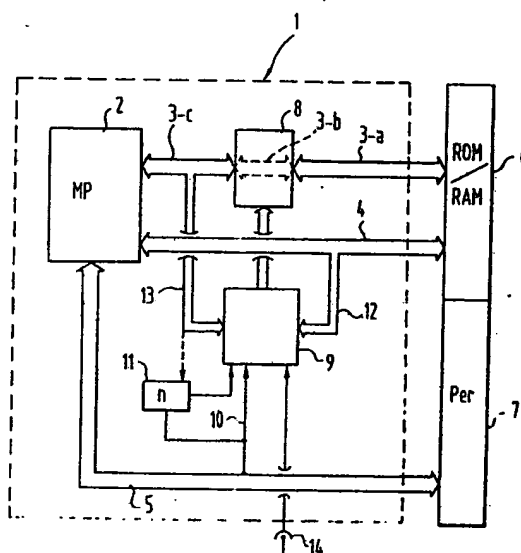
㉘ Vertreter:
Haft, U., Dipl.-Phys., 8000 München; Berngruber, O.,
Dipl.-Chem. Dr.rer.nat., 8232 Bayerisch Gmain;
Czybulka, U., Dipl.-Phys., Pat.-Anw., 8000 München

㉙ Erfinder:
gleich Anmelder

Prüfungsantrag gem. § 44 PatG ist gestellt

㉚ Datenschützender Standard-Mikroprozessor

Die Erfindung bezieht sich auf einen daten- bzw. programmschützenden Standard-Mikroprozessor (1) mit einer internen Dechiffrierschaltung (8, 9) zur Entschlüsselung und Bearbeitung von Daten, die von einem externen Programm- und Arbeitsspeicher (6) verschlüsselt angeboten werden. Um die Entschlüsselung eines mit hohem Aufwand erarbeiteten Programms zuverlässig zu verhindern, wird gemäß der Erfindung vorgeschlagen, daß die interne Dechiffrierschaltung (8, 9) in Abhängigkeit eines Befehlsabrufsignales (Op-Code-Fetch) und gegebenenfalls weiterer befehlsergänzender Signale sowie Programm- und Verarbeitungsdaten, die verschlüsselt angebotenen Daten selektiv erkennt, entschlüsselt und bearbeitet. Zur Ver- und Entschlüsselung werden mehrere Substitutionstabellen als Schlüssel verwendet, auf die in Abhängigkeit verschiedener Kriterien umgeschaltet wird.



DE 3432721 A1

3432721

11202 ch

Rüdiger Hahn
Raintalerstr. 39
8000 München 90

Datenschützender Standard-Mikroprozessor

Patentansprüche

1. Datenschützender Standard-Mikroprozessor, insbesondere zum Schutz eines Anwenderprogrammes mit einer internen Dechiffrierschaltung zur Entschlüsselung von verschlüsselt angebotenen Daten, dadurch gekennzeichnet, daß die interne Dechiffrierschaltung (8, 9) Steuereingänge (10, 11, 12, 13, 14) für ein Mikroprozessor-internes Befehlsabrufsignal (Op-Code-Fetch), gegebenenfalls befehls ergänzende Signale, Programm- oder Verarbeitungsdaten aufweist, und daß die Dechiffrierschaltung (8, 9) bei Vorliegen eines Steuersignales selektiert aktivierbar ist.
2. Mikroprozessor nach Anspruch 1, dadurch gekennzeichnet, daß die interne Dechiffrierschaltung (8, 9) interne Falltürschlüssel (8) lediglich für die während eines Befehlsabrufsignales (Op-Code-Fetch) angeforderten Operationsbefehlsteile aufweist, und daß die Dechiffrierschaltung (8, 9) lediglich während eines Op-Code-Fetch-Signales aktiviert ist.

3. Mikroprozessor nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die interne Dechiffrierschaltung (8, 9) mit dem internen Falltürschlüssel (8) Steuereingänge (10, 13) für das Op-Code-Fetch-Signal und befehlsergänzende Signale aufweist, und daß die Dechiffrierschaltung für die durch den Op-Code-Fetch repräsentierten Operationsbefehlsteile und die durch die befehlsergänzenden Signale repräsentierten befehlsergänzenden Daten unterschiedliche Schlüssel anbietet.
4. Mikroprozessor nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die interne Dechiffrierschaltung (8, 9) mit den internen Falltürschlüsseln (8) einen Steuereingang (13) aufweist, der ein Signal entsprechend Datenteilen eines Anwenderprogrammes, insbesondere Tabellen repräsentiert, und daß über diesen Steuereingang ein zusätzlicher, auf die Datenteile des Anwenderprogrammes angewendeter Schlüssel aktivierbar ist.
5. Mikroprozessor nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die interne Dechiffrierschaltung (8, 9) mit den internen Falltürschlüsseln (8) einen vorwählbare Datenverarbeitungsbereiche eines Anwenderprogrammes repräsentierenden Steuereingang (13) aufweist, wobei die Daten in den vorwählbaren Bereichen des Anwenderprogrammes verschlüsselt angeboten, entschlüsselt bearbeitet und gegebenenfalls wieder verschlüsselt werden, und daß die Informationszuführung zu der internen Dechiffrierschaltung (8, 9) hinsichtlich der Lage der Datenteile des Anwenderprogrammes intern (Steuerleitung 13) vorwählbar oder über zusätzliche externe Mikroprozessoranschlüsse (Steuereingang 14) möglich ist.

6. Mikroprozessor nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die interne Dechiffrierschaltung (8, 9) mit den internen Falltürschlüsseln (8) einen Speicher- und Logikbereich für einen freien Substitutions-Code zur Verfügung stellt, und daß die dem Mikroprozessor (1) angebotenen Daten nach diesem Substitutions-Code verschlüsselt sind.
7. Mikroprozessor nach Anspruch 6, dadurch gekennzeichnet, daß im Speicher- und Logikbereich (8) der internen Dechiffrierschaltung (8, 9) mehrere Falltürschlüssel gespeichert sind, deren Substitutionen den angebotenen, verschlüsselten Daten entschlüsselt entsprechen, und daß die interne Dechiffrierschaltung (8, 9) eine Steuerschaltung (9) mit mehreren Steuereingängen (10, 11, 12, 13) aufweist, über die eine Umschaltung auf jeweils einen anderen Falltürschlüssel möglich ist.
8. Mikroprozessor nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die interne Dechiffrierschaltung (8, 9) eine Vorschlüssel- und Steuerschaltung (9) aufweist, die aus zugeführten Steuersignalen (10, 11, 12, 13, 14) einen Vorschlüssel bildet, und daß der Ausgang der Steuerschaltung (9) mit einem Aktivierungseingang des Speicher- und Logikbereiches (Schlüsselspeicher 8) verbunden ist.
9. Mikroprozessor nach Anspruch 8, dadurch gekennzeichnet, daß die mit einem Steuereingang der Steuerschaltung (9) verbundene Steuerleitung (10) für das Op-Code-Fetch-Signal außerdem über einen Zähler (11) mit einem weiteren Steuereingang der Steuerschaltung (9) verbunden ist.

10. Mikroprozessor nach Anspruch 9, dadurch gekennzeichnet, daß der Eingang des Zählers (11) zusätzlich über eine Abzweigung (13) mit dem internen Datenbus (3-i) des Mikroprozessors (1) verbunden ist, um in Abhängigkeit aufeinanderfolgender befehlsergänzender Daten, aufeinanderfolgender Programmtabellen oder Programmdateien entsprechend des dadurch weitergeschalteten Zählerstandes jeweils einen anderen Falltürschlüssel anzu-steuern.
11. Mikroprozessor nach einem der Ansprüche 7 bis 10, da-durch gekennzeichnet, daß zur Umschaltung auf einen anderen Falltürschlüssel (8) zumindest ein Teil der Leitungen des Adressbus (4), auf dem das verschlüssel-te Datum im Anwenderprogramm angeboten wird, mit einem Steuereingang (12) der internen Dechiffrierschaltung (8, 9) verbunden ist.
12. Mikroprozessor nach einem der Ansprüche 7 bis 11, da-durch gekennzeichnet, daß zumindest ein Teil der Daten-leitungen des Datenbus (3-a, 3-i), auf denen verschlüs-selte Datenworte angeboten werden, über eine Abzwei-gung (13) mit einem Steuereingang der internen De-chiffrierschaltung (8, 9) verbunden sind.
13. Mikroprozessor nach einem der Ansprüche 7 bis 12, da-durch gekennzeichnet, daß die interne Dechiffrier-schaltung (8, 9) zusätzliche Steuereingänge (14) auf-weist, über die externe Kriterien zur Umschaltung auf andere Falltürschlüssel (8) zuführbar sind.
14. Mikroprozessor nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Mikroprozessor (1) eine Hybridschaltung ist.

15. Mikroprozessor nach einem der Ansprüche 1 bis 13, dadurch gekennzeichnet, daß der Mikroprozessor (1') als monolithische Schaltung aufgebaut ist.
16. Verfahren zum Verschlüsseln und Entschlüsseln eines Anwenderprogrammes mit Hilfe eines datenschützenden Mikroprozessors nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die in dem Anwenderprogramm nicht genutzten und im Mikroprogramm des Mikroprozessors nicht belegten Operationsbefehle innerhalb einer Substitutionstabelle für einen angewendeten Schlüssel mehrfach belegt werden.
17. Verfahren zum Verschlüsseln und Entschlüsseln eines Anwenderprogrammes mit Hilfe eines datenschützenden Mikroprozessors nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß zur Ver- und Entschlüsselung mehrere Substitutionstabellen als Schlüssel oder zumindest Teile davon festgelegt werden, und daß die Reihenfolge der Substitutionstabellen bzw. Tabellenteile variiert wird.
18. Verfahren nach einem der Ansprüche 16 und 17, dadurch gekennzeichnet, daß die durch ein Op-Code-Fetch-Signal repräsentierten Programmbefehle nach einem anderen Schlüssel als sonstige Datenteile der Operationsbefehle bzw. befehlsergänzende Daten verschlüsselt und entschlüsselt werden.

- 1 Die Erfindung bezieht sich auf einen datenschützenden Standard-Mikroprozessor gemäß dem Oberbegriff des Patentanspruches 1.
- 5 Die Einführung und weltweite Akzeptanz einiger weniger Standard-Mikroprozessoren für jeweils definierte Leistungsanforderungen resultiert aus der gleichen Interessenlage von Herstellern und Abnehmern. Durch die Massenfertigung, ermöglicht durch einen breiten Einsatzbereich,
10 sind günstige Preise möglich bei Standardisierung der Hardware und Anwendungsmodifikationen in der Software. Ebenso sind Standardisierungen in der Know-How-Vorbereitung und der Modulbereitstellung von Software für wiederkehrende Aufgabenstellungen bis hin zur Software-Bibliothek
15 ken möglich.

Eine solche Standardisierung hat jedoch Nachteile: Die Entwicklungskosten verlagern sich immer mehr von der Hardware zur Software, die vielfach nicht ausreichend ge-
20 schützt ist, so daß mit Kauf eines Gerätes mit einem Standard-Mikroprozessor das spezielle Know How weitergegeben wird und gegebenenfalls kopiert werden kann. Der Aufwand für die Entwicklung kundenspezifischer Software ist sehr hoch und erfordert in der Regel mehrere hundert-
25 tausend Mark. Die Know How-Verbreitung beim Einsatz weniger Standard-Mikroprozessoren vergrößert den Personenkreis ständig, der in Mikroprozessor-gesteuerten Geräten unerwünschte Manipulationen vornehmen kann. Außerdem sind Lizenzproduktionen, speziell im Ausland, aufgrund der be-
30 nötigten standardisierten Bauelemente nicht kontrollierbar. In jüngster Zeit wurden zur Vermeidung dieser Nachteile verschiedene Problemlösungen vorgeschlagen, so z.B. der Zugang zur Software über ein persönliches Paßwort, Vorsehen von internen Monitorprogrammen, die gegebenen-
35 falls programmierbar sind oder andere Maßnahmen zur Individualisierung der Hardware. Diese Vorschläge sind jedoch in der Regel nicht ausreichend, die Software zu schützen. In einigen Fällen werden sogar die eingangs ge-

1 schilderten Vorteile des Standard-Mikroprozessors aufgehoben.

Es wäre wünschenswert, einen Standard-Mikroprozessor mit
5 Hilfe von internen Schlüsseln und interner Dechiffrierlogik zu modifizieren, um so dem jeweiligen Anwender zu erlauben, Programme und hilfsweise auch Daten seines assembliert bzw. kompiliert vorliegenden Programmes bzw. auch der Daten im Originalspeichermedium dem Mikroprozessor
10 verschlüsselt anzubieten und dadurch Kopieren der Hardware und Software bzw. eine Manipulation in Mikroprozessor-Schaltungen unmöglich zu machen. Die physikalischen und geometrischen Eigenschaften des Original-Mikroprozessors sollten weitestgehend erhalten bleiben. Ebenso sollte das
15 erworbene Entwicklungs-Know-How mit dem entsprechenden Original-Mikroprozessor nutzbar bleiben. Die dem Original-Mikroprozessor einprägbaren Schlüssel individualisieren dabei die Hardware und Software, wobei alle Standardisierungsmerkmale der Hardware-Schaltungen bzw. der Software-
20 Module beibehalten werden. Eine mit einem solchen datenschützenden Mikroprozessor geschützte Schaltung ist in der Original-Hardware ablauffähig, wobei der Original-Mikroprozessor durch den datenschützenden Mikroprozessor und das originale Anwenderprogramm bzw. die Anwenderdaten
25 durch die verschlüsselte Entsprechung substituiert werden.

In der internationalen Patentanmeldung RS/65894/CH ist
- vorgeschlagen worden, die Daten in Programm- und Arbeitsspeicher zu verschlüsseln und diese bei der Bearbeitung
30 durch den Mikroprozessor durch Einschalten einer Dechiffrierschaltung in den Datenbus zwischen Speicher und Mikroprozessor wieder zu entschlüsseln. Ver- und Entschlüsselung erfolgen dabei so, daß die Positionen der einzelnen Datenleitungen innerhalb des Datenbusses planmäßig zwischen dem Speicher
35 und dem Mikroprozessor vertauscht werden. Diese Vertauschung erfolgt demnach nach Art eines Kreuzschienenverteilers: Ist der Datenbus z. B. eine Acht-Bit-Datenleitung, so werden zwischen Eingang und Ausgang der Dechiffrier-

1 schaltung die einzelnen, jeweils ein Bit tragenden Daten-
leitungen entsprechend dem verwendeten Schlüssel vertauscht.
Hierbei ist noch die Möglichkeit vorgesehen, mehrere Schlüs-
sel zu verwenden, wobei diese Schlüssel dann adressabhängig
5 sind.

Dieses Verfahren und die damit zusammenhängende Mikropro-
zessorschaltung macht sich eine Erkenntnis zunutze, die
z. B. für Nachrichtenverbindungen aus der US-PS 3546380
10 oder aus dem IBM Technical Disclosure Bulletin, Band 19,
Nummer 12, Mai 1977, Seiten 4564 ff bekannt ist. Die
übermittelten Daten werden entweder seriell oder
parallel in ihrer Position innerhalb eines Blockes, z. B.
eines Bytes vertauscht.

15 Auch wenn hierdurch ein Datenschutz in gewissem Umfange
gewährleistet ist, so bietet dieses Verfahren keine
Sicherheit vor einer Kopierung. Nicht zuletzt liegt dies
daran, daß sämtliche Daten aus dem Programm- und Arbeits-
20 speicher, die dort verschlüsselt vorliegen, über die
Dechiffrierschaltung laufen und dort entschlüsselt werden.
Durch die simple Vertauschung der Positionen der einzelnen
Bits innerhalb eines Bytes erscheinen sowohl in dem ver-
schlüsselten als auch entschlüsselten Datenwort immer die
25 gleiche Anzahl von EINSen und NULLen. Außerdem meldet
der Mikroprozessor über den Adressbus dem Programm- und
Arbeitsspeicher Rückinformationen, so z. B. Zwischener-
gebnisse bei sogenannten JUMP-Befehlen. Aus dem anschlie-
ßend verschlüsselt aus dem Programm- und Arbeitsspeicher
30 ausgesendeten Daten können hier wieder Rückschlüsse auf
die tatsächlichen Daten und damit auch auf die Verschlüs-
selungsmethode gezogen werden. Durch diese Art der Ver-
und Entschlüsselung erhält ein Fachmann, der die Mikro-
prozessorschaltung auch hinsichtlich der Software kopieren
35 will, eine Vielzahl von Informationen, die ihm die Ent-
schlüsselung erleichtern.

1 Der Erfindung liegt die Aufgabe zugrunde, einen Standard-Mikroprozessor so zu modifizieren, daß insbesondere Programmdaten gegen Kopieren zuverlässig geschützt sind.

5 Diese Aufgabe ist gemäß der Erfindung durch die im kennzeichnenden Teil des Patentanspruches 1 angegebenen Merkmale gelöst.

Weitere Ausgestaltungen der Erfindung gehen aus den

10 Unteransprüchen hervor.

Der programm- bzw. datenschützende Standard-Mikroprozessor beinhaltet zusätzlich zu dem Original-Standard-Mikroprozessor eine interne Schlüssel/Vorschlüssel-Dechiffrier-
15 schaltung, nach deren Durchlauf der Original-Prozessoranteil des datenschützenden Mikroprozessors das angebotene verschlüsselte Datum erkennt und bearbeitet. Die Ver- und Entschlüsselung erfolgt entsprechend der Hardware des Original-Mikroprozessors nach folgenden Kriterien:

20

a) Op-Code eines Befehles, d.h. derjenige Befehlsteil, der den Befehl definiert und der mit einem Befehlsabrufsignal, dem sogenannten Op-Code-Fetch abgerufen wird;

25 b) Datenanteil eines Befehls;

c) Datenanteil eines Programmes, z.B. die Tabellen;

d) Datenverarbeitungsbereiche eines Programmes, die im Bereich des Arbeitsspeichers RAM abgelegt sind.

30 Die Schlüssel/Vorschlüssel-Dechiffrierschaltung erkennt diese Kriterien und bearbeitet die Daten separat mit zugeordneten individuellen Schlüsseln, z.B. den Schlüsseln A, B, C bzw. D.

35 Um die Anzahl der verfügbaren Schlüssel multiplikativ zu erhöhen, stehen weiter folgende Kriterien des Anwenderprogrammes zur Verfügung:

- 1 1) Das Datenwort selbst;
- 2) die Adresse, auf welcher das Datenwort appliziert wird;
- 3) die Ordnungszahl des Datenwortes bei Mehrfachzugriffen zusammenhängender Daten;
- 5 4) extern zugeführte individuelle Hard- oder Software-Kriterien.

Auf diese Weise werden z.B. die Schlüssel A-1, A-2, ..., A-n, B-1, B-2, ..., B-n, ..., D-n definiert. Hiermit sind viele eindeu-
10 tigen Kriterien zuzuordnende Schlüssel möglich. Vorzugsweise werden nur die Op-Codes der Befehle, die mit dem Op-Code-Fetch abgerufen werden, nach einem freien Substitutions-Code verschlüsselt und entsprechend dechiffriert. Die übrigen Daten können unverschlüsselt vorliegen. Zur
15 Verschlüsselung und Entschlüsselung werden die oben angegebenen Kriterien herangezogen. Die Anzahl der möglichen Verschlüsselungen ergibt sich durch eine Permutation der Speicherplätze des Mikroprozessors, bei herkömmlichen Mikroprozessoren bei 256 Speicherplätzen demnach 256!. Der
20 freie Substitutions-Code kann z.B. so gewählt werden, daß die Eingangs- und Ausgangsdaten der Dechiffrierschaltung nicht die gleiche Anzahl von EINS- UND NULL-Bits aufweisen. Es ist im übrigen nicht notwendig, sämtliche Substitutionstabellen der verwendeten Schlüssel in der De-
25 chiffrierschaltung zur Verfügung zu stellen. Vielmehr ist es aufgrund der oben genannten Kriterien möglich, aus den Substitutionstabellen entsprechende Bereiche auszuwählen, wodurch trotz der gleichen Anzahl von verwendeten Schlüsseln die Speicherkapazität und damit auch die Hardware-
30 Ausführung der Dechiffrierschaltung verkleinert werden kann.

Die Vorschlüssel/Schlüsseltechnik gemäß der Erfindung, die an den oben genannten Kriterien ausgerichtet ist, erlaubt eine Optimierung der zusätzlich im Mikroprozessor benötigten Hardware.
35

Werden z.B. zwei Adressleitungen A0 und A1 als Schlüssel-

- 1 Multiplikator im obigen Sinne verwendet, so wären dadurch jeweils vier Schlüssel angesprochen. Der angesprochene Schlüssel ist durch die Ordinalzahlen 1 bis 4 der Adressstellen des angebotenen verschlüsselten Datums fixiert.
- 5 Wird zusätzlich das Kriterium: Ordinalzahl der Stellen des Datenwortes verwendet, wobei ein Zweistufenzähler mit vier Stellen unterstellt ist, ergeben sich bereits 16 verschiedene Schlüsselmöglichkeiten.
- 10 Es kann nun der Schlüsselbedarf optimiert werden, indem beispielsweise nur vier Schlüssel X0 bis X4 eingegeben werden. Dabei beeinflusst das zweite Kriterium (Ordinalzahl des Datenwortes) die stringent zugeordnete Ordinalzahl des ersten Kriteriums, d.h. der Adresse. Im vorliegenden
- 15 Beispiel ergeben sich für die vier durch Adresszuordnung eindeutig fixierten Schlüssel X0 bis X4 durch Verwendung des zusätzlichen Kriteriums Ordinalzahl des Datenwortes $4! = 24$ Ordnungsschemata für die Schlüsselfolge, d.h. die Schlüsselfolgen X1-X2-X3-X4; X2-X4-X3-X1;....usw.
- 20 Die eindeutige Zuordnung der Schlüsselfolge durch das Adresskriterium wird damit aufgehoben. Wenn ansonsten durch die Multiplikation der zur Verfügung stehenden Schlüssel entsprechend der Kriterien Adressabhängigkeit und Datenwortabhängigkeit 16 Schlüssel zumindest teilweise
- 25 tabellarisch gespeichert werden müßten, so brauchen durch die Aufhebung der eindeutigen Zuordnung nur vier Schlüssel wiederum zumindest nur teilweise zur Verfügung gestellt zu werden. Der Hardware-Bedarf von 12 Zusatzschlüsseln ist durch Wegfall der eindeutigen Zuordnungsmöglich-
- 30 keiten kryptografisch kompensiert.

Es gibt ferner eine einfache Möglichkeit, bei Verwendung von Substitutionstabellen als Schlüssel diese unregelmäßig zu gestalten: Mikroprozessoren nutzen nämlich im all-

35 gemeinen nicht den gesamten zur Verfügung stehenden Raum des Mikroprozessors für Operationsbefehle, so daß von vorneherein einige Kombinationen leer sind. Außerdem werden in vielen Programmen nicht alle durch den Mikroprozessor

- 1 möglichen Operationsbefehle ausgenutzt. Diese nicht ge-
nutzten Kombinationen innerhalb des Mikroprozessors bzw.
des Anwenderprogrammes können als Löcher bezeichnet wer-
den. Derartige Löcher können innerhalb der Substitutions-
5 tabelle mehrfach belegt werden. Dem verwendeten Schlüs-
sel liegt dann keine echte Permutation sämtlicher Opera-
tionsbefehle zugrunde, sondern eine Permutation mit Mehr-
fachbelegungen, wodurch die Entschlüsselung weiterhin er-
schwert wird.
- 10
Damit ist der jeweils angesprochene Schlüssel nach dem
individuellen Anwenderprogramm optimierbar.
- Ein daten- insbesondere programmschützender Standard-
15 Mikroprozessor gemäß der Erfindung kann in Hybridtechnik
ausgeführt werden. Eine solche Ausbildung hat den Vorteil,
daß die Schaltung auch gegen sogenannte harte Angriffe
gesichert werden kann, bei denen versucht wird, den
mechanischen Aufbau des Prozessors direkt zu kopieren.
- 20
Ein daten- und programmschützender Standard-Mikroprozes-
sor kann jedoch auch dadurch realisiert werden, daß die
Schlüssel direkt in das Mikroprogramm des Mikroprozessors
eingeschrieben werden, so daß ein monolithischer Chip ge-
25 schaffen wird, der praktisch nicht kopierbar ist. Auch wenn
dann z.B. das verschlüsselte Programm aus dem Programm-
speicher kopiert wird, ist es nicht möglich, dieses Pro-
gramm mit einem herkömmlichen Mikroprozessor zu betreiben.
- 30 Eine Schaltung, bestückt mit einem programmschützenden
Standard-Mikroprozessor gemäß der Erfindung ist demnach
durch Individualisierung der Hardware - indem der Original-
Mikroprozessor durch einen programmschützenden Prozessor
ersetzt wird - und Verschlüsseln der Software wirksam ge-
35 schützt.

Weitere Ausgestaltungen der Erfindung gehen aus den Unter-
ansprüchen hervor. Die Erfindung ist in zwei Ausführungs-

1 beipielen anhand der Zeichnung näher erläutert. In der
Zeichnung stellen dar:

Figur 1 ein Blockschaltbild eines programmschützenden
5 Mikroprozessors, das auf einem Modul eines handels-
üblichen Original-Mikroprozessors basiert, wobei
dieser programmschützende Mikroprozessor in Hybrid-
technik ausgeführt ist;

10 Figur 2 ein Blockschaltbild eines programmschützenden
Mikroprozessors gemäß der Erfindung, das auf einer
Spezialausführung eines handelsüblichen Original-
mikroprozessors basiert und in diesem Falle in
monolithischer Technik hergestellt ist.

15 Ein programmschützender Mikroprozessor (1) weist als
Kernstück einen Standard-Mikroprozessor (2) auf, z. B.
einen Mikroprozessor Z80, der über einen internen Daten-
bus 3-i, einen externen Datenbus 3-a, beides 8-Bit-Daten-
20 leitungen, ferner über einen Adressbus 4 und Steuerleitun-
gen 5 mit Daten arbeitet. Der programmschützende Mikro-
prozessor arbeitet mit einem externen Programm- und Arbeits-
speicher 6, der aus einem Festwertspeicher ROM, in dem die
Programmdaten enthalten sind, und einem Arbeitsspeicher RAM
25 zur Speicherung von Zwischenergebnissen und dergleichen zu-
sammengesetzt ist, sowie mit weiteren Peripheriebau elemen-
ten 7 zusammen. Externer und interner Datenbus 3-a bzw. 3-i
sind über einen ansteuerbaren Schlüsselspeicher 8 mitein-
ander verkoppelt. Für den Schlüsselspeicher ist ein hier
30 noch intern gestrichelt gezeichneter Bypass 3-b vorgesehen,
der die Daten auf dem Datenbus 1:1 durchläßt, sofern der
Schlüsselspeicher nicht angesteuert ist, und dieses auch
im reinen Lese- und Schreibbetrieb zum Mikroprozessor
und vom Mikroprozessor weg tut.

35 Der Schlüsselspeicher, der auch als Logikschaltung auf-
gebaut sein kann, wird durch das Op-Code-Fetch-Signal
aktiviert, das ein Signal der Steuerleitungen ist bzw.

- 1 aus den Signalen der Steuerleitungen entwickelt werden
kann. Dieses Op-Code-Fetch zeigt an, daß der Mikroprozessor 2
einen Operationsbefehl anfordert, z. B. JUMP, ADDIEREN, etc.
- 5 Der Schlüsselspeicher 8 wird durch eine Vorschlüssel- und
Steuerschaltung beeinflusst. In dem Programmspeicher ROM
sind die den Op-Code-Fetches zugeordneten Operationsbe-
fehle für den Mikroprozessor verschlüsselt abgelegt.
Zur Darstellung der Operationsbefehle werden meist hexa-
10 dezimale Zahlen (Hex-Zahlen) aus dem 16 "Ziffern" 0, 1, 2,
..., 9, A, B, ..., F verwendet, so daß ein Byte durch
zwei Hexziffern angegeben wird. Die Hexzahl F2 entspricht
der Bitfolge 1 1 1 1 0 0 1 0. Das Befehlsregister eines
8-Bit-Mikroprozessors beinhaltet demnach maximal 16 x
15 16 = 256 Bytes, in Hexschreibweise die Bytes 0 0, 01, ...,
FF, sofern der Mikroprozessor auf 1-Byte-Operationsbefehle
beschränkt ist. Sind Mehr-Byte-Operationsbefehle vorge-
sehen, die durch Op-Code-Fetches repräsentiert werden,
multipliziert sich die Anzahl der zur Verfügung stehenden
20 Befehle im Befehlsregister entsprechend. Jede Befehlsta-
belle kann zur Verschlüsselung entsprechend der Kombina-
tionsrechnung in eine andere permutierte Befehlstabelle
überführt werden. Eine derartige Permutation ist z. B. die,
daß die Hexziffern 0 bis 7 durch die Hexziffern 8 - F und
25 die Hexziffern 8 - F durch die Hexziffern 0 - 7 ersetzt
werden. Insgesamt sind hier bei jeder Befehlstabelle
256! Permutationen möglich. Jeder dieser Permutationen
ist eine Befehlstabelle zugeordnet, die eine bestimmte
Schlüsselnummer erhalten kann. Der verwendete Schlüssel
30 dient zur Verschlüsselung der durch Op-Code-Fetches re-
präsentierten Operationsbefehle des Anwenderprogrammes.
Die Vorschlüssel- und Steuerschaltung 9 sorgt dafür, daß
bei Abruf der einzelnen verschlüsselten Operationsbefehle
diese für den Mikroprozessor entschlüsselt werden. Die Ent-
35 schlüsselung erfolgt nur dann, wenn das Befehlsabrufsig-
nal (Op-Code-Fetch) anliegt.

- 1 Bei der Schlüsselsteuerung durch den Op-Code-Fetch alleine kann nur einer der 256! Schlüssel für den gesamten Adressraum des Anwenderprogrammes wirken, wenn nicht nach jedem Op-Code-Fetch auf einen anderen Schlüssel umgeschaltet
- 5 wird. Die Anzahl der verwendbaren Schlüssel kann jedoch durch verschiedene zusätzliche Kriterien vervielfacht werden. Hierzu ist eine Vorschlüssel- und Steuerschaltung 9 vorgesehen, die auf den Schlüsselspeicher 8 wirkt. Die Steuerschaltung 9 wird durch den Op-Code-Fetch über eine
- 10 von dem Steuerbus 5 abzweigende Steuerleitung 10 aktiviert und aktiviert dann ihrerseits den Schlüsselspeicher 8. Ein weiterer Steuereingang der Steuerschaltung 9 ist mit dem Ausgang eines n-stelligen Zählers 11 verbunden, dessen Eingang ebenfalls von der Op-Code-Fetch-Leitung 10 beauf-
- 15 schlägt wird. Diese Zuführung des Op-Code-Fetch zusätzlich über den n-stelligen Zähler 11 ermöglicht die Umschaltung des verwendeten Schlüssels bei Mehrbyte-Operationsbefehlen. Ein weiterer Steuereingang der Steuerschaltung 9 ist mit einer Abzweigung 12 von dem Adressbus 4 verbunden. Der
- 20 Steuerschaltung wird die jeweils anliegende Adresse bzw. ein Teil dieser Adresse über diese Abzweigung 12 zugeführt. Außerdem wird einem weiteren Steuereingang der Steuerschaltung 9 über eine Abzweigung 13 von dem internen Datenbus 3-i das gerade anhängige Datenwort bzw. ein Teil dieses
- 25 Datenwortes zugeführt. Die Leitung 13 kann noch - in Figur 1 gestrichelt dargestellt - mit dem Eingang des Zählers 11 verbunden werden, um gegebenenfalls eine Schlüsselumschaltung in Abhängigkeit weiterer Daten, wie befehlsergänzender Daten, Tabellendaten usw. zu ermöglichen. Außerdem kann
- 30 über einen zusätzlichen externen Ausgang 14 noch ein externes Kriterium einem weiteren Steuereingang der Steuerschaltung 9 zugeführt werden. Die der Steuerschaltung 9 zugeführten Steuersignale werden bei Anliegen eines Op-Code-Fetch an der Leitung 10 miteinander verknüpft. Durch
- 35 diese Verknüpfung wird der jeweilige Schlüssel bestimmt, der für die Entschlüsselung des Programmoperationsbefehls notwendig ist.

- 1 Es ist nicht notwendig, im Schlüsselspeicher 8 sämtliche durch diese Verknüpfung möglichen permutierten Befehls-substitutionstabellen zur Verfügung zu stellen. Durch Zuführung eines Teiles der Operationsbefehle über die
- 5 Datenabzweigung 13 zur Steuerschaltung 9 brauchen nur Teilbereiche der verwendbaren Schlüssel im Schlüsselspeicher 8 vorgesehen werden. Die Anzahl der tatsächlich verwendeten Schlüssel bleibt hierbei gleich, hingegen ist eine Schlüsseloptimierung möglich. Schlüsselspeicher 8 und
- 10 Steuerschaltung 9 bilden gemeinsam die Dechiffrierschaltung.

- In Figur 2 ist ein Blockschaltdiagramm für einen nach dem gleichen Prinzip arbeitenden, jedoch monolithisch aufgebauten Mikroprozessor 1' dargestellt, der gemäß der Er-
- 15 findung modifiziert ist. Der Mikroprozessor 1' kommuniziert über einen externen Datenbus 3'-a, einen Adressbus 4' und einen Steuerbus 5' mit seiner Peripherie. Über den unidirektionalen Adressbus 4' bestimmt der Mikroprozessor den zu aktivierenden Teil der Peripherie. Über den bidirektio-
- 20 nalen externen Datenbus 3'-a werden Daten ausgetauscht. Dabei liefert der Steuerbus 5' die notwendigen Steuerinformationen, z. B. die Richtung des beabsichtigten Datenflusses.
- 25 Der externe Datenbus 3'-a ist über ein Datenbus-Interface 21 mit dem internen Datenbus 3'-i verbunden. Der interne Datenbus 3'-i dient zum Informationsaustausch zwischen dem Datenbus-Interface und einem Arbeitsregister -Array 22 in beiden Richtungen, ferner zum Informationsaustausch
- 30 zwischen diesem Arbeitsregister-Array 22 und einer internen Rechen- und Logikschaltung (ALU) 23 sowie zum Informationsaustausch zwischen externen Datenbus 3'-a und einem internen Befehlsregister 24. Der Ausgang des Befehlsregisters 24 ist mit einem Befehlsdecodierer 25 verbunden,
- 35 der seine Informationen an eine Ablaufsteuerung 26 der zentralen Prozessoreinheit (CPU) liefert.

- 1 Der Schlüsselspeicher bzw. die Schlüssellogik 8' ist im
internen Datenbus 3'-i vorgesehen. Angesteuert wird der
Schlüsselspeicher 8' wiederum von einer internen Steuer-
schaltung 9', die als Steuergrößen für die Schlüsselum-
5 schaltung vom Adressbus 4' über eine Abzweigung 12' von
einem Zähler 11' für den Op-Code-Fetch, über einen externen
zusätzlichen Anschluß 14' und eine Datenleitungsabzweigung
13' Eingangssignale erhält, die bei Vorliegen eines von
der CPU-Ablaufsteuerung 26 über eine Leitung 10' abge-
10 zweigten Op-Code-Fetch-Signales aktiviert wird und dann
ihrerseits den Schlüsselspeicher 8' einschaltet.

Die Arbeitsweise dieses Mikroprozessors bei der Dechiffrie-
rung der verschlüsselt angebotenen Programmdateien ist iden-
15 tisch wie bei dem obigen Ausführungsbeispiel, so daß sich
eine nähere Erläuterung erübrigt.

Als Variante der in Figur 2 gezeigten Version kann das
Befehlsregister 24 selbst als Schlüsselspeicher ausgeführt
20 werden.

25

30

35

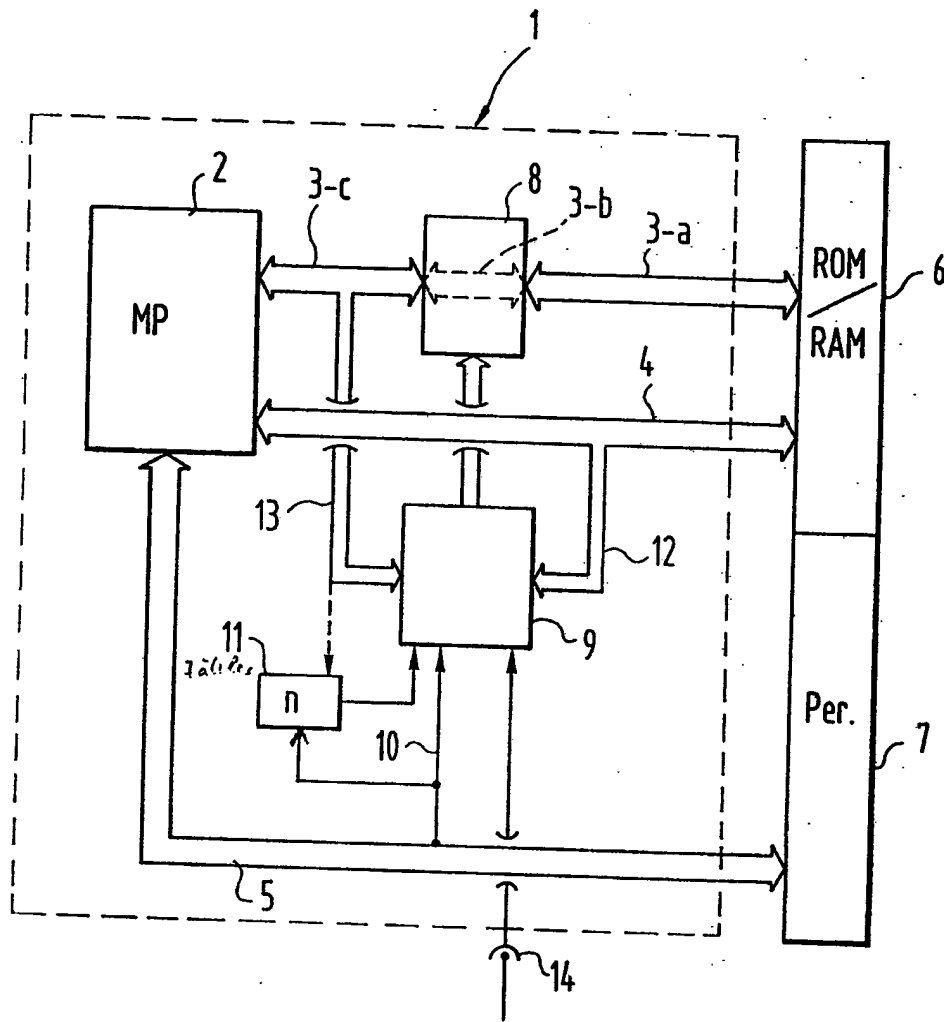


FIG. 1

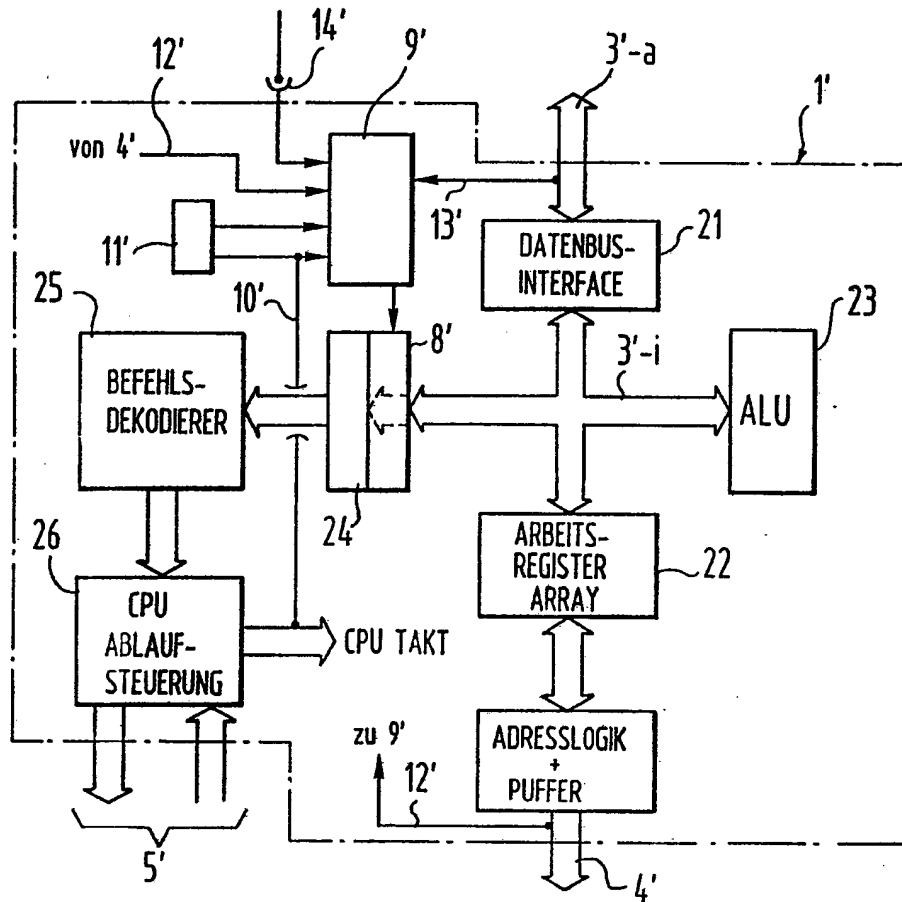


FIG. 2



P.B.5818 - Patentaan 2
2280 HV Rijswijk (ZH)
☎ +31 70 340 2040
TX 31651 epo nl
FAX +31 70 340 3016

Europäisches
Patentamt

Zweigstelle
in Den Haag
Recherchen-
abteilung

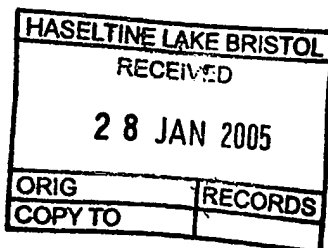
European
Patent Office

Branch at
The Hague
Search
division

Office européen
des brevets

Département à
La Haye
Division de la
recherche

O'Connell, David Christopher
Haseltine Lake,
Redcliff Quay
120 Redcliff Street
Bristol BS1 6HU
GRANDE BRETAGNE



Datum/Date

28.01.05

Zeichen/Ref./Réf.

P102005EP00/SJR

Anmeldung Nr./Application No./Demande n°/Patent Nr./Patent No./Brevet n°.
04255590.4-2212-

Anmelder/Applicant/Demandeur/Propriétaire/Propriétaire/Titulaire
Via Technologies, Inc.

COMMUNICATION

The European Patent Office herewith transmits as an enclosure the European search report for the above-mentioned European patent application.

If applicable, copies of the documents cited in the European search report are attached.

☐ Additional set(s) of copies of the documents cited in the European search report is (are) enclosed as well.

The following specifications given by the applicant have been approved by the Search Division:

☒ abstract

☒ title

☐ The abstract was modified by the Search Division and the definitive text is attached to this communication.

The following figure will be published together with the abstract: 3



REFUND OF THE SEARCH FEE

If applicable under Article 10 Rules relating to fees, a separate communication from the Receiving Section on the refund of the search fee will be sent later.





| DOCUMENTS CONSIDERED TO BE RELEVANT | | | |
|--|--|---|--|
| Category | Citation of document with indication, where appropriate, of relevant passages | Relevant to claim | CLASSIFICATION OF THE APPLICATION (Int.Cl.7) |
| X | US 5 666 411 A (MCCARTY JOHNNIE C) 9 September 1997 (1997-09-09) * abstract; figures 7-12 * * column 4 - column 23 * | 1-28 | G06F1/00 |
| X | "IBM PCI Cryptographic Coprocessor CCA Basic Services Reference and Guide for IBM 4758 Models 002 and 023 with Release 2.40" IBM, September 2001 (2001-09), XP002291430 * the whole document * | 1-28 | |
| X | EP 1 298 518 A (TOKYO SHIBAURA ELECTRIC CO) 2 April 2003 (2003-04-02) * the whole document * | 1-28 | |
| X | EP 1 202 150 A (TOKYO SHIBAURA ELECTRIC CO) 2 May 2002 (2002-05-02) * abstract; figures 1-15 * * paragraph '0017! - paragraph '0153! * | 1-28 | |
| X | US 4 633 388 A (CHIU MING-YEE) 30 December 1986 (1986-12-30) * the whole document * | 1-28 | TECHNICAL FIELDS SEARCHED (Int.Cl.7) |
| X | DE 34 22 721 A (HAHN RUEDIGER) 6 March 1986 (1986-03-06) * abstract; figures 1,2 * * page 6 - page 17 * | 1-28 | G06F |
| The present search report has been drawn up for all claims | | | |
| Place of search | | Date of completion of the search | Examiner |
| Munich | | 19 January 2005 | Nazzaro, A |
| CATEGORY OF CITED DOCUMENTS | | | |
| X: particularly relevant if taken alone Y: particularly relevant if combined with another document of the same category A: technological background O: non-written document P: intermediate document | | T: theory or principle underlying the invention E: earlier patent document, but published on, or after the filing date D: document cited in the application L: document cited for other reasons &: member of the same patent family, corresponding document | |

ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.

EP 04 25 5590

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
 The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

19-01-2005

| Patent documents cited in search report | | Publication date | Patent family member(s) | Publication date |
|--|---|---------------------|----------------------------|---------------------|
| US 5666411 | A | 09-09-1997 | NONE | |
| EP 1298518 | A | 02-04-2003 | JP 2003108442 A | 11-04-2003 |
| | | | CN 1410876 A | 16-04-2003 |
| | | | EP 1298518 A2 | 02-04-2003 |
| | | | US 2003065933 A1 | 03-04-2003 |
| EP 1202150 | A | 02-05-2002 | JP 2002140236 A | 17-05-2002 |
| | | | EP 1202150 A2 | 02-05-2002 |
| | | | US 2002051536 A1 | 02-05-2002 |
| US 4633588 | A | 30-12-1986 | EP 0155399 A2 | 25-09-1985 |
| DE 3432721 | A | 06-03-1986 | DE 3432721 A1 | 06-03-1986 |

EPO FORM P0469

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

THIS PAGE BLANK (USPTO)